

EXHIBIT 7



IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON

CONFIDENTIAL

**FRCP 26(a)(2)(B) Rebuttal Expert
Report of Kevin T. Faulkner**

HUNTERS CAPITAL, LLC, et al
vs.
CITY OF SEATTLE,

Case No. 2:20-cv-00983 TSZ



Introduction

Engagement Background

Palo Alto Networks, Inc. ("Palo Alto Networks") was initially retained by outside counsel on behalf of its client, the City of Seattle (the "City") on November 5, 2020, to provide digital forensic investigative services in connection with pending and anticipated litigation, including *Hunters Capital, LLC, et al v. City of Seattle*, No. 2:20-cv-00983 (W.D. Wash. 2020). The Unit 42 Security Consulting group ("Unit 42") at Palo Alto Networks, formerly known as the Crypsis Group, performed the services in this engagement.

I, Kevin T. Faulkner, have been asked to serve in an expert witness capacity by counsel for the City. On February 11, 2022, I submitted my report entitled "FRCP 26(a)(2)(B) Expert Report of Kevin T. Faulkner" (hereafter, my "Opening Report"). On April 28, 2022, Brandon Leatha, an expert witness for Hunters Capital, et al., submitted an expert report entitled "Expert Report of Brandon Leatha" (hereafter, the "Leatha Report"). I have been asked to review and respond to the opinions and other statements made in the Leatha Report, and hereby submit my Rebuttal Expert Report.

When I refer to actions taken by myself or Unit 42 in this report, those actions were taken by me and/or Unit 42 personnel who were working at my direction. All dates and times discussed in this report are presented in Coordinated Universal Time ("UTC"), unless otherwise noted.

Experience and Qualifications

My background, experience, and qualifications are disclosed in the "Experience and Qualifications" section and Exhibit 1 of my Opening Report, which I incorporate herein.

In addition to the experience documented in my Opening Report, I have now testified as an expert in an additional trial in The United States District Court for the Northern District of California. Attached to this report as Exhibit 1 is an updated true and correct copy of my curriculum vitae, which sets forth a detailed list of my background, qualifications, and testimony experience.

Compensation

As explained in my Opening Report, Palo Alto Networks is being compensated for my work on this case at the rate of \$550 per hour for my professional services in this matter. Certain members of my team at Unit 42 who are working at my direction on this matter are billing between \$300 and \$550 per hour. Palo Alto Networks also charges \$700 per hour for expert testimony. Neither Palo Alto Networks' nor my compensation depends in any way on the outcome of this matter or the substance of my opinions or testimony.

Materials Considered

The materials that I considered in forming the opinions set forth in this report include my over 18 years of experience as a digital forensics expert, the Leatha Report, my Opening Report, all materials considered in my Opening Report, all references cited in this report, and the list of materials attached as Exhibit 2 to this report.

Reservation of Rights

I reserve the right to supplement or amend my opinions or this report at any time prior to the expert disclosure deadlines in the case, in response to opinions expressed by other experts, or in light of any additional evidence, testimony, discovery, court rulings, or other information that may be provided to me after the date of this report. In addition, I reserve the right to consider and testify about issues that may be raised by fact witnesses and experts at trial.



In connection with any testimony that I am asked to provide in this matter, I may use as exhibits various documents produced in this matter that refer or relate to the topics discussed in this report. In addition, I reserve the right to use animations, demonstratives, enlargements of exhibits, and other information to convey my opinions and the bases for them, as appropriate.

Summary of Opinions in This Report

The following is a summary of my opinions in rebuttal to the Leatha Report with following sections providing more details about my opinions related to former Seattle Mayor Jenny A. Durkan (“Mayor Durkan”), former Seattle Police Chief Carmen Best (“Chief Best”), Seattle Fire Chief Harold Scoggins (“Chief Scoggins”), Idris Beauregard, Christopher Fisher, Kenneth Neafcy, and Seattle Police Assistant Chief Eric Greening (“Asst. Chief Greening”). Also included are sections on Retention Requirements, Access to Locked iPhone Data, iPhone Functionality, and Factual Errors.

I reviewed the Leatha Report and identified a number of statements about text messages being deleted that do not consider if those text messages were separately preserved on other occasions and/or from other devices or repositories. Several mobile devices were preserved multiple times, and the same text messages were preserved from multiple custodians in this matter. Statements about the numbers of text messages deleted from any one given data source that do not consider all available data sources do not provide an accurate account of what was actually preserved and produced.

In addition, the Leatha Report seems to frame any deletion activity as a failure to preserve something the City or its employees had an obligation to preserve. Based on sworn testimony from the City Records Manager, Jennifer Winkler, City employees do not have an obligation to retain all text messages. In fact, the City advised employees to use text messaging only for “transitory” messages which then “can be deleted.”

Retention Requirements

On Page 5 of the Leatha Report, after bullet points summarizing claimed losses of text messages, the report states, “The actions outlined above each resulted in the loss of text messages that the City had an obligation to preserve.” This statement is misleading, as one might understand this to mean that the City had an obligation to preserve all of the messages that the Leatha Report claims were deleted, even though the Leatha Report does nothing to establish what obligations the City may have had in regards to data preservation. Ultimately, what obligations the City did or did not have in preserving text messages is a legal conclusion and not an expert opinion in the area of digital forensics. From reviewing the deposition transcript of Jennifer Winkler dated January 6, 2022, I do understand that the City Records Manager testified that her office prepared the City’s advice documentation for text messages and it does not require the retention of every message.¹ Exhibit 2 of Ms. Winkler’s deposition is the advice documentation for text messages, entitled “CRMP Advice Sheet for Text Messages,” which states, “An employee should limit texting regarding City business to transitory texts that can be deleted once the message serves its purpose.”² It further states, “The retention period for public records depends on the function and content of the record, not its format or method of transmission. How long text messages need to be kept depends on the information transmitted within the text. Having just one blanket retention period for text messages is akin to having a single retention period for all letter-sized paper - the format does not determine the retention.”³ The document also states, “‘Transitory’ text means a text message that only documents information of temporary, short-term value, and that is not needed as evidence of a business transaction”⁴ and, “Transitory texts may be deleted by the user once the texts have served their purpose.”⁵

¹ Jennifer Winkler 1/6/2022 Depo. Tr. at 17:12-19:17 and 21:17-24:11.

² See SEA_00148109

³ *Id.*

⁴ *Id.*

⁵ See SEA_00148110



The document also gives examples of transitory text messages, below are the examples listed:⁶

- Texts that set work meetings or request job-related phone calls.
- Texts that are akin to voice mail messages.
- Texts noting the sender has completed a simple task (e.g. "I returned the call to Mary Smith," "The broken water main has been repaired," or "The suspect has been apprehended.")
- Texts informing a coworker/supervisor that the sender will be late to work, late to a meeting, is taking the day off, or another similar message.
- Texts that ask another employee to take some form of simple action (e.g. "Can you please take your City vehicle to the shops," "I need you to call Frank about the sewer line on 256th," or "You are needed in court at 11:00 a.m.")
- Texts that contain information that is later included in another City record. Examples include:
 - A Street Supervisor receives a text from a coworker informing him of a fallen tree on 256th Street. The Supervisor later prepares a work report noting the fallen tree on 256th, and that he sent a crew to clean up the tree. Once the work report is prepared, the text becomes transitory.
 - A Police Detective receives a text from a Sergeant explaining that she talked with a witness in an investigation and asking the Detective to follow up and take a statement from the witness. The Detective then takes a statement from the witness. Once the statement is taken, the text becomes transitory.

I also am aware of, and have reviewed, a document titled "Mayor's Office Best Practices" that is dated June 19, 2020, that discusses the Public Records Act and contains a section regarding the preservation of text messages. In the "Text Message" section, it states "It is the responsibility of each City employee to retain public records, including those on City-owned or personal smartphones and mobile devices. Retention of text messages is based on the content of the message and the function it documents, not the method of transmission. Retention policies can range from immediate deletion for transitory records to several years based on the content."⁷

Access to Locked iPhone Data

On Page 5, the Leatha Report claims, "If a technical issue prevented the City Officials from accessing their phones, a temporary replacement should have been issued instead of factory resetting and deleting all the data." This statement is misleading, as it implies that someone made a conscious choice regarding resetting a City employee's phone. While resetting an iPhone can be done by a user choosing the menu options to initiate a reset, it can also occur upon entering the incorrect passcode too many times if the option to "Erase Data" is enabled. This option will automatically "Erase all data on [an] iPhone after 10 failed passcode attempts." The Leatha Report has not shown that each City employee chose to reset their phone as opposed to simply entering the incorrect passcode too many times with this "Erase Data" option enabled.

Even when iPhones that are locked with an unknown or forgotten passcode are preserved, gaining access to the text message data on the device is not certain. The Leatha Report states on Page 5 that, had the locked phone been preserved, "A qualified digital forensic vendor could then have assisted with preserving the data." Leatha's statement is misleading because a digital forensic vendor may not be able to extract data from an iPhone with an unknown passcode. Standard digital forensic tools used to extract data from iPhones require the passcode to be entered into the iPhone in order to extract and preserve text message

⁶ See SEA_00148109

⁷ See SEA_00144659



data from the iPhone models that were reset in this matter. Even with more advanced tools that are not widely available to digital forensic vendors, which are capable of cracking or bypassing the passcodes on iPhone devices, the process is not guaranteed to succeed and an attempt can run for weeks or months without success. This process could also be very expensive, especially if undertaken for every City employee who is ever locked out of their phone. It should not be assumed that, had a passcode-locked iPhone been provided to digital forensic vendors, that they would have been able to access any available text message data.

When a digital forensic vendor can access a passcode-locked iPhone, this access does not necessarily give them the ability to recover every text message ever sent or received on that iPhone. Generally, a digital forensic vendor will be able to extract the active text message information and, possibly, limited deleted text message information from an iPhone. Therefore, the total number of text messages sent or received is not necessarily lost when an iPhone is factory reset; rather, only the text messages still present on or recoverable from a given iPhone may be lost if they are not available from other sources when a factory reset occurs.

Mayor Durkan

The Leatha Report characterizes the factory reset process for Mayor Durkan's iPhone 8 Plus (FirstNet) in a way that is inconsistent with my understanding of the events that took place.

Page 13 of the Leatha Report states, "On September 17, 2020, Durkan's iPhone 8 Plus (FirstNet) was factory reset a second time." While my analysis concluded that this iPhone was factory reset on September 17, 2020, PDT, it cannot be determined that this was the "second time." I have reviewed the deposition transcript of Emmanuel Arhu, a City IT employee, who was asked under oath what he did with the iPhone 8 Plus (FirstNet) (referred to in the deposition as "the old iPhone with the cracked screen") after it was replaced. In his deposition, Mr. Arhu testified, "...our standard operating procedure, I just hold on to it, and that's what we do pretty much with everyone else in the City that we work on their devices. We hold on to it for a few weeks just to make sure that everything works for them, so -- in case they come back to ask for something, we can go back and verify. So I held on to it for, I believe, about four weeks. That's what we normally do before wiping them."⁸ Mr. Arhu states that he factory reset this iPhone about four weeks after it went out of use on July 9, 2020, which would be on or about August 7, 2020. This is prior to the iTunes back-up of Mayor Durkan's iPhone 11 (Plus) that was taken on August 21, 2020. Based on Mr. Arhu's deposition testimony, the factory reset on September 17, 2020, PDT may not have been the second time that the device was factory reset. It is also possible that a factory reset process that was initiated on or about August 7, 2020, was incomplete and that September 17, 2020, PDT represents the next time the iPhone was powered on and the process completed. The Leatha Report has not substantiated its claim that this was specifically the "second time."

The Leatha Report also makes several statements about Mayor Durkan's text messages that are misleading. When considering messages from multiple mobile devices and multiple preservasions of those mobile devices, providing analysis from one preservation without considering the others provides an incomplete picture of the messages that were preserved and are available.

Page 14 of the Leatha Report states, "All messages between ROWID 165 and 5,912 are missing, indicating that the 30-day retention setting deleted 5,746 messages that were dated prior to June 25, 2020, at 10:38am PDT." It is accurate that all messages between ROWID 165 and 5,912 are not present in the data extractions specifically from Mayor Durkan's iPhone 11 (FirstNet), but this statement is misleading in that the majority of these 5,746 messages are available from other sources. For example, the iPhone 8 Plus (Verizon) included 3,845 active messages dating from November 18, 2017, through October 30, 2019. Also, Volume 3 of the text message reconstruction for Mayor Durkan includes 7,550 text message records that were preserved from multiple mobile device sources prior to June 25, 2020, at 10:38 a.m. PDT. The text message reconstruction for Mayor Durkan does include duplicate text message records when the

⁸ Emmanuel Arhu 3/3/2022 Depo. Tr. at 71:11-71:23.



messages were reconstructed from more than one mobile device that was involved in the same text message exchange, which would have to be factored out to arrive at the number of unique text messages represented in the reconstruction. Between the dates of October 30, 2019, at 02:05:49 (where data on the iPhone 8 Plus (Verizon) ends) and June 25, 2020, at 17:38:48 (where the data on the iPhone 11 (FirstNet) begins), there are 1,562 entries in the text message reconstruction for Mayor Durkan. As stated above, the reconstruction does include duplicates when the messages were reconstructed from more than one mobile device that was involved in the same text message exchange.

These messages from the iPhone 8 Plus (Verizon) and from the text message reconstruction for Mayor Durkan constitute a significant majority of the 5,746 messages that were not available in the data extraction from Mayor Durkan's iPhone 11 (FirstNet). Without considering these other sources of text message data, one might incorrectly assume that the 5,746 messages deleted were actually lost and not otherwise preserved and produced.

Figure 6 on Page 15 of the Leatha Report is a table that lists the numbers of text messages from multiple preservasions of mobile devices used by Mayor Durkan. Figure 6 includes a column named "Deleted Messages as % of Total," which contains percentages of messages deleted compared to the total message count from each preservation. These percentages appear to be correctly calculated, but are misleading as they do not consider text message data available from other sources, including other sources listed within Figure 6 itself. The numbers and percentages listed as deleted for the iPhone 11 (FirstNet) in Figure 6 do not factor in the messages still active on the iPhone 8 Plus (Verizon) listed on Figure 6, nor do these numbers factor in the text messages in the text message reconstruction for Mayor Durkan. Again, without considering all the sources of text message data, one might incorrectly assume that the numbers and percentages listed as deleted were actually lost and not otherwise preserved and produced.

With respect to the "sms.db" on Mayor Durkan's iPhone 11 (FirstNet), the Leatha Report states, "My analysis of the ROWID gaps in the message table shows that an additional 191 messages were manually deleted between June 25, 2020, and November 16, 2020." (Leatha Report, Page 14). There are 191 ROWID gaps in the "Message" table, but this statement is misleading in that the majority of these 191 messages are available from other sources. Twenty of these 191 messages are available from other copies of Mayor Durkan's iPhone 11 (FirstNet) that were taken prior to November 2020. Another 111 of these 191 messages are available in Volume 3 of the text message reconstruction for Mayor Durkan. Therefore, in total, at least 131 of these 191 messages are available from other sources. I understand that the City's text message reconstruction efforts are ongoing and, therefore, the number of reconstructed messages may continue to increase. I also understand that other reconstructed text messages may have been withheld for various reasons (e.g., because they are privileged), meaning that the number recovered could be even higher than just what can be found in these data sources. Factoring in the messages withheld would be necessary in order to fully evaluate how many of the 191 messages have been identified in other sources, but it will be at least 131 of 191, or over 68 percent. To put these 191 messages into additional context, in this same time frame, Mayor Durkan's iPhone 11 (FirstNet) had a total of 2,416 messages, of which 191 or just under 8 percent were deleted. At least 131 of these messages were recovered from other sources, leaving 60 messages out of 2,416 total messages, or a bit over 2 percent, that have not yet been reconstructed from other sources.

In addition, as described in the "Retention Requirements" section of this report, above, not all text messages are required to be retained. The Leatha Report does not demonstrate that any of these 191 deleted text messages were of the type that needed to be retained.

Chief Best

Page 16 of the Leatha Report states, "...the Microsoft Teams, Twitter, Facebook, and LinkedIn applications were also installed on Best's iPhone XS Max." This is incorrect. While artifacts relating to these applications are present on Chief Best's iPhone XS Max, none of these applications are installed. This is consistent with these applications having been installed at an earlier point in time on Chief Best's iPhone XS Max or even on a prior iPhone used by Chief Best.



Page 16 of the Leatha Report also says that Leatha's analysis "...indicates that 27,138 messages had been deleted from Best's iPhone XS Max." While the arithmetic is correct, the conclusion is not. These 27,138 deleted messages were not "...deleted from Best's iPhone XS Max" but rather were deleted from across all of the iPhones used by Chief Best for as long as she was working for the City and transferring text message data from one iPhone to another when upgrading phones.

Page 17 of the Leatha Report, under the heading of "Evidence of ESI Available from Other Sources (former Chief Best)" states, "I did not identify any additional sources of data likely to contain Best's missing text messages that had not been collected and identified on the ESI Log provided by the City." For Chief Best's iPhone XS Max, the Cellebrite forensic software lists a "Sync host name" in the file "iTunesPrefs" that identified that iTunes had been synchronized and/or backed up to "Computer: OC510093\User: colint"; however, the Leatha Report did not identify this additional source of potentially relevant electronically stored information ("ESI"). I understand from the City that this computer named OC510093 was issued to "Tricia Colin," a City employee whose username is "colint." Ms. Colin's computer included two iTunes backups of iPhones previously used by Chief Best; an iPhone 6s Plus backed up on November 15, 2017; and an iPhone 8 Plus backed up on October 1, 2019. The iPhone 8 Plus shows that it was set up as a new phone, without data being restored from an earlier phone, starting on November 5, 2018, based on the creation of a number of system databases. The oldest message in the "sms.db" database on this backup of the iPhone 8 Plus is a message with ROWID 3, dated November 6, 2018. This message does not have a text message body; it is a message with an "item_type" of "1," which is an internal database entry created when a group chat occurs. The iPhone 8 Plus was backed up and then restored to Chief Best's iPhone XS Max on October 1, 2019. That backup and restore process is further evidenced by artifacts such as the "DataUsage.sqlite" database on the iPhone XS Max, which has entries going back to November 5, 2018 that match entries in the "DataUsage.sqlite" database from the iPhone 8 Plus.

Based on the backup and restore of Chief Best's iPhone 8 Plus to her iPhone XS Max, the 27,138 deleted messages dating back to November 6, 2018, were actually deleted from Chief Best's iPhone 8 Plus and her iPhone XS Max. The most recent text message on the iPhone 8 Plus is dated October 1, 2019, and has a ROWID of 10,319. This means that 10,319 of the 27,138 deleted messages were dated on or before October 1, 2019.

Additionally, it is misleading to say that "...27,138 messages had been deleted from Best's iPhone XS Max" when many of those messages are available from other sources. The text message reconstruction for Chief Best consists of 1,697 total text message records sent or received just in the 33 day window between June 8, 2020, and July 10, 2020, that were preserved from multiple mobile device sources. The text message reconstruction for Chief Best does include duplicate text message records when the messages were reconstructed from more than one mobile device that was involved in the same text message exchange. Without considering all the sources of text message data, one might incorrectly assume that the 27,138 messages were all in a relevant time frame when, actually, they stretch back to late 2018. Also, without considering all the sources of text message data, one might incorrectly assume that all messages in the period of June 8, 2020, to July 10, 2020, that were deleted were actually lost and not otherwise preserved, when numerous messages are actually available from other sources. Furthermore, I understand that the City's text message reconstruction efforts are ongoing and, therefore, the number of reconstructed messages may continue to increase.

Christopher Fisher

Page 18 of the Leatha Report states, "The City reported that on approximately December 3, 2020, Fisher experienced an issue with the facial recognition functionality on his iPhone 7, and that he did not remember his passcode." I understand the date reported by the City to have been approximate. As the Leatha Report also states on Page 18, "The com.apple.MobileBackup.plist configuration file contained a RestoreDate key set to '11/3/2020 12:52:14 AM' and the WasCloudRestored key set to 'True'." I understand that additional discussion with Mr. Fisher revealed that he recalled the lock-out and restore of his phone occurred in the late fall of 2020, but did not recall the precise date—i.e. while he initially believed he was locked out on December 3, 2020, it is possible that he actually was locked out on November 3, 2020.



I also understand that the City's initial representation, as stated on Page 18 of the Leatha Report, that "...Fisher experienced an issue with the facial recognition functionality on his iPhone 7..." resulted from a miscommunication over the type of "biometric" feature Fisher used to access his iPhone, with the City later correcting the statement on May 19, 2022, to say that "Fisher attempted to gain access to his phone using the bio-metric functionality that he usually used to access his phone."⁹ It further states, "That bio-metric functionality was the thumbprint capability that iPhone 7's utilized."¹⁰

My understanding is that Mr. Fisher had no City-issued device other than his iPhone 7 throughout the summer of 2020. The document numbered SEA_00174043 shows that Mr. Fisher later received a newer iPhone XR on December 9, 2020.

Mr. Fisher's iPhone 7 was logged in with the Apple ID [Redacted] " which I understand to be Mr. Fisher's personal Apple ID. The iTunes Store on Mr. Fisher's iPhone 7 was logged in with the Apple ID [Redacted], " which I understand to be Mr. Fisher's City Apple ID. Because Mr. Fisher's City-issued iPhone 7 was synchronizing photos¹¹ with his personal Apple ID, any photos synchronized to his iCloud account from his personal devices would also be synchronized to his City-issued iPhone 7.

Page 19 of the Leatha Report describes three models of iPhones found based on analysis of metadata in photos that includes the model of phones used to take various pictures. I understand these three iPhones to be personal devices of Mr. Fisher. Because his personal photos were synchronizing with his City-issued iPhone 7, this information about Mr. Fisher's personal devices was present on his City-issued device.

Also on Page 19, the Leatha Report describes finding two different phone numbers for Mr. Fisher in text message communications with other City employees and in some iPhone configuration files. I understand the phone number [Redacted] to be Mr. Fisher's personal mobile phone number and [Redacted] to be Mr. Fisher's City mobile phone number.¹² I also understand that the City has recently learned that Mr. Fisher did use his personal mobile device for some text message communications with other City employees and that the City is taking steps to try to obtain any relevant text messages from Mr. Fisher.

On Page 18, the Leatha report states, "15,843 messages had been deleted from Fisher's iPhone 7." It is misleading to say 15,843 messages were deleted when some of those messages are available from other sources. Also, because Mr. Fisher's iPhone 7 was restored from a backup after it had been factory reset, all text messages available in that backup would have been restored onto the iPhone 7.

The text message reconstruction for Chris Fisher includes a total of three messages for the [Redacted] mobile phone number between June 10, 2020, and July 27, 2020, that were preserved from multiple mobile device sources. The text message reconstruction for Chris Fisher also includes a total of 341 entries for the [Redacted] mobile phone number between June 10, 2020, and July 31, 2021, that were preserved from multiple mobile device sources. The text message reconstruction for Chris Fisher does include duplicate text message records when the messages were reconstructed from more than one mobile device that was involved in the same text message exchange. I understand that the City's text message reconstruction efforts are ongoing and, therefore, the number of reconstructed messages may continue to increase.

Kenneth Neafcy

On Page 21, the Leatha Report says that the factory reset of Neafcy's iPhone XS on October 27, 2020, resulted in "the loss of all text messages that he sent or received between March 19, 2020, and October

⁹ Plaintiffs' Second Set of Interrogatories to Defendant City of Seattle and The City's Objections and Amended Response to Interrogatory No. 31, dated May 19, 2022.

¹⁰ See *Id.*

¹¹ The file "cpl_enabled_marker" was present on Mr. Fisher's iPhone 7. This demonstrates that syncing of photos was enabled on this device.

¹² SEA_00174043



28, 2020.” It is misleading to say that all text messages during that time period were lost when some of those messages are available from other sources.

The reset activity described on Page 21 of the Leatha Report is consistent with the City’s earlier interrogatory answers regarding Neafcy’s devices. The City’s First Supplemental Answer to Interrogatory No. 31 for Kenneth Neafcy states, “During the relevant period, Neafcy was using an iPhone X. On or about October 26, 2020, Neafcy was prompted by the City’s periodic security protocol installed on his iPhone that he needed to change his passcode for accessing the phone. Neafcy followed the instructions to reset the passcode. He then tried to access the phone using the passcode that he had just input, but it did not work. He is not sure whether he mistyped the passcode when he set it or whether another issue with his phone occurred. After he was not able to access his phone, he contacted IT and asked for assistance. IT proposed ways to access the phone, but none of them was successful. He tried to recover the phone from iCloud, but it sent the passcode to the phone that was locked so he could not view it. Because of the upcoming November 2020 election and the need for others to reach him, Neafcy removed the SIM card from his iPhone X and inserted it into an old iPhone 8, allowing him to go back to using his iPhone 8 for work purposes. The City has imaged the iPhone X, and concluded that no text messages exist from the period during which Neafcy was using it.”¹³

The “iPhone X” described in the City’s statements is more accurately described as an iPhone XS, and the “iPhone 8” described in the City’s statements is more accurately described as an iPhone 6s. Furthermore, in the City’s First Supplemental Answer to Interrogatory No. 23 for Kenneth Neafcy, when the City says that “Neafcy’s phone did not have texts on it pre-dating approximately October 26, 2020,”¹⁴ it would be more accurate to say that Neafcy’s phone did not have texts on it predating October 28, 2020, from the summer or fall of 2020. Neafcy’s iPhone 6s does contain text messages from June 15, 2017, to March 20, 2020.

The text message reconstruction for Kenneth Neafcy includes a total of 1,683 entries for the [Redacted] mobile phone number between June 9, 2020, and May 29, 2021, that were preserved from multiple mobile device sources. Of those 1,683 entries, 1,249 are dated between June 9, 2020, and October 23, 2020, which represent the reconstructed messages within the date range listed in the Leatha Report. The text message reconstruction for Kenneth Neafcy does include duplicate text message records when the messages were reconstructed from more than one mobile device that was involved in the same text message exchange. I understand that the City’s text message reconstruction efforts are ongoing and, therefore, the number of reconstructed messages may continue to increase.

Chief Scoggins

On Page 24, the Leatha Report states that the factory reset of Chief Scoggins’ iPhone 8 Plus on October 8, 2020, resulted in “in the loss of all text messages prior to that date.” It is misleading to say that all text messages prior to October 8, 2020, were lost when some of those messages are available from other sources.

The text message reconstruction for Chief Scoggins consists of three separate reconstructions with a combined total of 20,069 entries dated from December 18, 2017, to March 9, 2021, for the [Redacted] mobile phone that were preserved from multiple mobile device sources. This includes 15,821 entries dated between December 18, 2017, and September 26, 2020. The text message reconstructions for Chief Scoggins include duplicate text message records when the messages were reconstructed from more than one mobile device that was involved in the same text message exchange. I understand that the City’s text message reconstruction efforts are ongoing and, therefore, the number of reconstructed messages may continue to increase.

¹³ Plaintiffs’ Second Set of Interrogatories to Defendant City of Seattle and the City’s Objections and First Supplemental Responses Thereto, No. 31.

¹⁴ Plaintiffs’ Second Set of Interrogatories to Defendant City of Seattle and the City’s Objections and First Supplemental Responses Thereto, No. 23.



The reset activity on October 8, 2020, described on Page 24 of the Leatha Report is also consistent with the City's earlier interrogatory answers regarding Chief Scoggins' device. The City's First Supplemental Answer to Interrogatory No. 31 for Chief Scoggins states, "During the relevant period, Chief Scoggins used an iPhone 8. On October 8, 2020, Chief Scoggins reported to the City's IT department and an assistant that he had been locked out of his phone. The City understands that, because of pre-existing City of Seattle security protocols, Chief Scoggins was required to enter a passcode in order to access the phone. Chief Scoggins entered what he believed to be the correct passcode, but it did not gain him access to the phone. He asked IT if they could help him unlock his phone, access to which is vital given his role as Fire Chief, and was advised to attempt to recover his iPhone from iCloud. As the City understands the situation, ultimately, he was not successful because the authentication code required to recover the phone was sent to the phone, which he still could not access. The City understands that Chief Scoggins tried to unlock his phone using other methods suggested but could not gain access. Ultimately, the City understands that Chief Scoggins then took his iPhone to the Apple Store at University Village to see if they could help him gain access to it. Because of Apple's Covid-19 policies at the time, Chief Scoggins was not allowed to enter the store to observe the Apple Store employees' efforts to gain access. The Apple Store was able to gain access to the phone, but it appears that the Apple Store employee did so by resetting it, which caused all of Chief Scoggins' text messages to be lost."¹⁵ The "iPhone 8" described in the City's statements is more accurately described as an iPhone 8 Plus.

Idris Beauregard

On Page 26, the Leatha Report states that, due to the factory reset of Idris Beauregard's iPhone 8 on October 9, 2020, it resulted in "the loss of all text messages prior to that date." It is misleading to say that all text messages prior to October 9, 2020, were lost when some of those messages are available from other sources.

The text message reconstruction for Idris Beauregard includes a total of 4,647 entries for the **Redacted** mobile phone number between June 16, 2020, and February 7, 2021, that were preserved from multiple mobile device sources. Of these 4,647 entries, 4,400 are dated prior to October 9, 2020. The text message reconstruction for Idris Beauregard does include duplicate text message records when the messages were reconstructed from more than one mobile device that was involved in the same text message exchange. I understand that the City's text message reconstruction efforts are ongoing and, therefore, the number of reconstructed messages may continue to increase.

The reset activity on October 9, 2020, described on Page 26 of the Leatha Report is also consistent with the City's earlier interrogatory answers regarding Beauregard's device. The City's First Supplemental Answer to Interrogatory No. 31 for Idris Beauregard states, "During the relevant period, Beauregard used an iPhone 8. The City understands that on October 9, 2020, Beauregard attempted to access his phone, but his passcode would not work. He does not believe that he had the wrong information for the passcode, as it was the one he had previously used. When he could not access his phone, he called IT and submitted a request for assistance (called a heat ticket). The City understands that Beauregard was informed by IT that, because it was an iPhone, he should contact Apple to see if they had a work-around that he could use. Apple informed him that because he did not have iTunes, he could not gain access to the phone. He left his phone on his desk with the idea that he would work to gain access the next day. However, the City understands that when he looked at his phone the next day, he saw that his iPhone screen showed a spiral icon. Once the spiraling stopped the phone reset itself. None of his text messages pre-dating the phone's automatic reset were available after the phone reset itself."¹⁶

¹⁵ Plaintiffs' Second Set of Interrogatories to Defendant City of Seattle and the City's Objections and First Supplemental Responses Thereto, No. 31.

¹⁶ *Id.*



Asst. Chief Greening

On Page 27, the Leatha Report states that the oldest available text message for Asst. Chief Greening's Samsung Galaxy S8 phone was "dated October 27, 2020, at 8:28 AM PDT" after the phone had been "factory reset on the morning of October 26, 2020, prior to 9:14 AM PDT." This suggests that all text messages prior to October 27, 2020, at 08:28 a.m. PDT were lost as a result of the factory reset on the prior day. This is misleading as some of those messages are available from other sources.

The text message reconstruction for Asst. Chief Greening includes a total of 481 entries for the [Redacted] [Redacted] mobile phone number between June 9, 2020, and June 25, 2021, that were preserved from multiple mobile device sources. Of these 481 entries, 327 are dated prior to October 27, 2020. The text message reconstruction for Asst. Chief Greening does include duplicate text message records when the messages were reconstructed from more than one mobile device that was involved in the same text message exchange. I understand that the City's text message reconstruction efforts are ongoing and, therefore, the number of reconstructed messages may continue to increase.

The reset activity on October 26, 2020, described on Page 27 of the Leatha Report also is consistent with the City's earlier interrogatory answers regarding Asst. Chief Greening's device. The City's First Supplemental Answer to Interrogatory No. 31 for Asst. Chief Greening states, "During the relevant period, Assistant Chief Greening used a Galaxy S8 phone. The City understands that Greening typically used the biometric (facial or finger recognition) feature of the phone to gain access. Greening was out on vacation the week of October 19, 2020. It is the City's understanding that at some point while he was out of the office or when he returned on Monday, October 26, the City's security protocols required that he input a passcode instead of using the biometric access feature. Greening made a few attempts to gain access using what he thought was his passcode to the phone, but none of the passcodes worked. Worried that the phone would reset if he tried too many times, Greening asked his assistant, Celina Villa, to take his phone to IT to see if they could gain access. He recalls providing her with the phone and receiving it back later that day or the next day. At that point, he was able to access the phone, but his text messages from before that date were no longer available. The City's belief is that SPD IT had to reset his phone because of the passcode issue."¹⁷

iPhone Functionality

In addition to points relevant to specific custodians, my review of the Leatha Report also identified a number of discrepancies or misleading statements about how different functions of iPhones work in general.

The Leatha Report states "For example, when turning 'Messages in iCloud' on or off, the KeepMessagesVersionID is incremented by 1. See Faulkner, 20-21." (Leatha Report, Page 9). This is only partly correct; the KeepMessagesVersionID increments when turning "Messages in iCloud" on, but not when turning "Messages in iCloud" off.

The Leatha Report states that "The sqlite_sequence table in the sms.db keeps track of the next available ID for certain tables." (Leatha Report, Page 10). This is incorrect; the "sqlite_sequence" table in the "sms.db" keeps track of the current ROWID for certain tables, not the next available ID.

The Leatha Report states, "If the 'Messages in iCloud' feature was once enabled, and subsequently disabled, the messages would be available in iCloud for 30 days after the feature was turned off." (Leatha Report, Page 12). This is incorrect. If the "Messages in iCloud" feature is simply disabled, the messages would remain available in iCloud beyond 30 days. Only the use of the "Disable & Delete" function will cause the copy of text messages in iCloud to be deleted after 30 days. This "Disable & Delete" function is separate from just turning off or disabling "Messages in iCloud." It is also important to note that using the "Disable & Delete" function does not affect the copy of text messages stored on the iPhone itself, only the copy stored

¹⁷ *Id.*



in iCloud. Thus, even if the “Disable & Delete” function is selected by a user, it will not cause the copies of locally stored messages on the user’s phone to be deleted after 30 days.

Footnote 15 of the Leatha Report states, “The CloudKitSyncingEnabled key from the com.apple.madrid.plist configuration file was set to “False”, indicating that the messages in iCloud feature was not used.” (Leatha Report, Page 20). This statement is incorrect and should be corrected to read “...indicating that the messages in iCloud feature was not *currently* used.” The CloudKitSyncingEnabled key only records the current setting and not historical settings that might have changed over time. Furthermore, “messages in iCloud” should be properly capitalized and read as “Messages in iCloud.”

Factual Errors

Finally, there are a number of factual errors I identified in my review of the Leatha Report. The more substantive of these are listed below.

Figure 2 in the Leatha Report on Page 7 lists “Source Date[s]” for the items with Evidence ID’s E045A and E049A as “8/17/2021” and “10/27/2021” respectively. Our analysis shows that these dates should be 08/16/2021 and 10/29/2021. These dates listed in the Leatha Report appear to be a typographical error or otherwise incorrect.

Footnote 15 of the Leatha Report states, “The sms.db - message table has 64 entries remaining, however only 16 were actual text messages and contained content.” (Leatha Report, Page 17). The correct number of text messages that contained content is 15 and not 16.

Footnote 22 of the Leatha Report states, “Dates can be stored in many different formats. The **LastCloudBackup** key is stored in Apple Absolute Time, which is the number of seconds that have elapsed since ‘2001-01-01 00:00:00 Z’.” (Leatha Report, Page 25). The Leatha Report identified an incorrect key, LastCloudBackup; the correct key is LastCloudBackupDate.

Dated: June 3, 2022

Respectfully submitted,

Kevin T. Faulkner